AO 106 (Rev. 04/010) Application for Search Warrant AUTHORIZED AND APPROVED/DATE: /S Bow Bottomly 11/30/2023

UNITED STATES DISTRICT COURT

for the

WESTERN DISTRICT OF OKLAHOMA

In the Matter of the Search of
(Briefly describe the property to be search
Or identify the person by name and address)
PROPERTY KNOWN AS:
8300 NW 10th St., Apt. 2
Oklahoma City, Oklahoma 73127

Case No: M-23- 973-SM

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property *(identify the person or describe property to be searched and give its location)*:

See Attachment A, which is attached and incorporated by reference.

Located in the Western District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized)*:

See Attachment B, which is attached and incorporated by reference.

The basis for the search under Fed. R. Crim.P.41(c) is (*check one or more*):

- ☒ evidence of the crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252A	Distribution of child pornography
18 U.S.C. § 2252A	Receipt of child pornography
18 U.S.C. § 2252A	Possession of child pornography

The application is based on these facts:

See attached Affidavit of Special Agent Shane Robinson, Federal Bureau of Investigations, which is incorporated by reference herein.

- ☒ Continued on the attached sheet(s).
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet(s).

Applicant's signature

SHANE ROBINSON
SPECIAL AGENT
FEDERAL BUREAU OF INVESTIGATIONS

Sworn to before me and signed in my presence.

Date: NOVEMBER 30, 2023

Judge's signature

City and State: Oklahoma City, Oklahoma

SUZANNE MITCHELL, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Shane Robinson, a Special Agent with the Federal Bureau of Investigation (FBI), Oklahoma City, Oklahoma, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent (SA) of the FBI since April 2023 and have been assigned to the Oklahoma City Division of the FBI, Norman Resident Agency. I have received training and consulted with other agents who have experience with cases involving child pornography and sexual exploitation of children.

2. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

3. The information contained in this Affidavit is based upon my personal knowledge and observation, my training, conversations with other law enforcement officers, and review of documents and records. This Affidavit is made in support of an application for a warrant to search the entire premises located at **8300 NW 10th St., Apt. 2, Oklahoma City, Oklahoma 73127** (hereinafter referred to as "the **SUBJECT PREMISES**"), which is described in detail in Attachment A to this Affidavit, including the residential dwelling, vehicles, curtilage, any persons located on said property, and any computer (as broadly defined in 18 U.S.C. § 1030(e)(1)) or other digital file storage device located there, for the items specified in Attachment B hereto, which constitute instrumentalities, fruits, and evidence of violations 18 USC § 2252A (possession, receipt, and distribution of child pornography).

4. This investigation, described more fully below, has revealed that an individual knowingly utilized Kik from the **SUBJECT PREMISES**, to receive, distribute, and possess, in violation of 18 U.S.C. § 2252A, and that there is probable cause to believe that evidence, fruits, and instrumentalities of such violations are located at the **SUBJECT PREMISES**.

5. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

TERMS

6. Based on the training and experience of other law enforcement officers with whom I have had discussions I use the following technical terms and definitions:

a. An Internet Protocol (IP) address is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static, or long-term, IP addresses. Other computers have dynamic, or frequently changing, IP addresses.

b. Internet Service Providers (ISPs) as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

c. Computer, as used broadly herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones. See 18

U.S.C. § 1030(e)(1).

d. Minor as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

e. Records, documents, and materials as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

CHARACTERISTICS COMMON TO INDIVIDUALS WITH INTENT TO COLLECT RECEIVE OR DISTRIBUTE CHILD PORNOGRAPHY

7. Based on the training and experience of other law enforcement officers with whom I have had discussions and my own research, I know there are certain characteristics common to individuals with intent to view and/or possess, collect, receive, or distribute images of child pornography:

a. Individuals with intent to view or possess, collect, receive, or distribute child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals with intent to view or possess, collect, receive, or distribute child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals with intent to view or possess, collect, receive, or distribute child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their films, videotapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain photos, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals with intent to view or possess, collect, receive, or distribute pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals with intent to view or possess, collect, receive, or distribute child pornography also may correspond with or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access online forums, such as bulletin boards, newsgroups, internet relay chat or chat rooms are considered more advanced users and therefore more experienced in acquiring and storing a collection of child pornography images.

8. Individuals with intent to view and/or possess, collect, receive, or distribute child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

BACKGROUND OF INVESTIGATION

9. This case originated on October 24, 2023, when your affiant received a lead from FBI Tampa Division, Sarasota Resident Agency. During their investigation, agents accessed a subject's cellular device. On this device were conversations from an unidentified Kik group, which appeared to focus on the trading of videos and pictures of child sexual abuse material (CSAM).

10. Kik is a social media smartphone application that can be used to exchange text, images, and videos. The app usually requires users to register a unique user screen name. The registration process for this app requires the user to provide contact information to register their screen name, such as an email address or phone number.

11. On or about April 28, 2023, the Kik username "Okcsparky" posted multiple CSAM thumbnail pictures to this Kik group. One of the unidentified users in this group commented "Anymore rough ones?", to which "Okcsparky" replied "Idk… I'm driven it's hard to look through my shit". After these comments, "Okcsparky" posted multiple CSAM thumbnail pictures to the group.

12. On August 14, 2023, FBI Tampa Division issued an administrative subpoena to Kik, to provide information pertaining to subscriber information and IP logs associated with the username "Okcsparky" (hereafter "the **SUBJECT ACCOUNT**") from April 27, 2023, to August 14, 2023.

13. On August 16, 2023, FBI Tampa Division received Kik's response to the administrative subpoena with the following information regarding **SUBJECT ACCOUNT**: email address: kraigvarney76@gmail.com; First Name: moving; Last Name: Left. On the date of the CSAM postings described in paragraph 11, the **SUBJECT ACCOUNT** utilized the IP address 68.12.212.15 to login to Kik. This IP address resolved to Cox Communications (Cox).

14. On August 31, 2023, FBI Tampa Division issued an administrative subpoena to Cox, to provide information pertaining to subscriber information associated to the following: IP address 68.12.212.15, Port: 36078, Date: 2023-04-28 19:57:31 UTC 68.12.212.15, Port: 58504, Date: 2023-04-28 19:59:55 UTC 68.12.212.15, Port: 58808, Date: 2023-04-28 20:01:46 UTC.

15. On September 11, 2023, FBI Tampa Division received Cox's response to the administrative subpoena with the following information regarding the subscriber of the IP address 68.12.212.15, on the requested timeframe described above:

Name:	Kelly Watson
Address:	8300 NW 10th St, Apt 2, Oklahoma City, Oklahoma 73127
Phone:	(405) 627-8919 (405) 761-1802
E-Mail:	kellyin.pink@gmail.com

16. A search of Oklahoma Department of Public Safety provided current driver's license photo and residential information for Kelly Watson (Watson) who resides at 8300 NW 10th St., Apt. 2, Oklahoma City, Oklahoma 73127.

17. On November 1, 2023, your affiant conducted an open-source search and identified a Facebook account for Kelly Watson who states on her account that she resides in Oklahoma City, Oklahoma. Upon review, there were multiple photos of Watson. The Facebook photos and the driver's license photo appear to show the same person, which is Kelly Watson. Furthermore, Watson's email address kellyin.pink@gmail.com is similar to Kelly Watson's Facebook account, www.facebook.com/kellyin.pink.

18. On November 1, 2023, your affiant searched the Oklahoma Department of Corrections (DOC) database for Kraig Varney (VARNEY). According to VARNEY's criminal history, he served time in prison for drug trafficking and firearms related charges. VARNEY, born October 3, 1976, had several booking photographs in the database, including one photograph which showed the upper portion of a tattoo on VARNEY's chest. VARNEY is pictured in numerous photographs on Watson's Facebook account, including one photograph that shows his chest tattoo from the DOC database.

19. Your affiant believes Kraig VARNEY is the owner and user of the email address kraigvarney76@gmail.com and that he used this email to register the **SUBJECT ACCOUNT** with Kik referenced in paragraph 13.

20. On October 25, 2023, FBI Tampa Division followed FBI CSAM protocols and securely transferred CSAM which was distributed by "Okcsparky" in a Kik group text. Your affiant reviewed all of the images/videos, including CSAM, provided by FBI Tampa Division. Based on the training and experience of other law enforcement officers and my own research, it was determined that several of the files depict children under the age of eighteen years engaged in sexual acts or lascivious exhibitions of the genitals that constitute child pornography as defined by Title 18 U.S.C. § 2256. A few of the files are described below:

a. Filename: c3546efd4c246975c86b886a4ab18e8b
Description: This image depicts a nude prepubescent female lying on her back with her legs spread open and up in the air. She has what appears to be a pencil shaped object in her hand penetrating her vagina. There appears to be an adult hand penetrating her anal cavity with an index finger.

b. Filename: 61ff8a7394609d6bcf2c88644cfb06d6
Description: This image depicts a prepubescent female, wearing what appears to be a swimsuit with pinkish purple and white stripes, laying on her back being penetrated by an erect penis while the male's hand is pressing down on her stomach.

c. Filename: d26f218b696fc17a05549d9c4d6ef84

Description: This image depicts a nude prepubescent female laying next to a nude adult male, both are lying on their backs, and another nude female is on her knees hovering over the male. The nude adult male has his arm wrapped around the nude prepubescent female with his hand placed on her vagina and his other arm is wrapped around the thigh of the nude female hovering over him.

d. Filename: 383cb4fd49ef0f9fld89dec217414784
Description: This image depicts a prepubescent female with her hands grabbing her butt as she places her index finger on her anal cavity, while a toothbrush is protruding upright out of her vagina.

21. Your affiant conducted postal checks and it was confirmed that VARNEY receives mail at 12324 South Land Avenue, Oklahoma City, Oklahoma, 73170. VARNEY does not receive mail at 8300 NW 10th St., Apt. 2, Oklahoma City, Oklahoma 73127. This application requests only to search 8300 NW 10th Street, Apt. 2, Oklahoma City, Oklahoma 73127, because this is where VARNEY was located at the time the CSAM was distributed and is believed to keep his smartphone, computer, and other electronic devices. Specifically, the Kik chats reveal that VARNEY was using his smartphone to distribute and view child pornography in April of 2023 and it is common knowledge that smartphone users almost always have their smartphones near them.

22. On November 7, 2023, your affiant interviewed M.O., VARNEY's probation officer, at Department of Corrections, 1919 Industrial Boulevard, Norman, Oklahoma 73069. M.O. provided VARNEY's cellular telephone number, (405) 679-8310 (**SUBJECT CELLPHONE**), and his employment information at Oklahoma Electrical Supply Company, located in Tulsa, Oklahoma. M.O. contacts VARNEY via the **SUBJECT CELLPHONE** to schedule Home Visits and in person visits at Department of Corrections, Norman, Oklahoma.

23. On November 9, 2023, a search warrant for the information associated with the cellular device assigned call number (405) 679-8310 in the custody or control of T-Mobile was issued by United States Magistrate Judge Amanda Maxfield Green. On November 13, 2023, your

affiant began receiving pings. Your affiant has observed those pings in the close vicinity of the **SUBJECT PREMISES** 10 out of the last 16 days.

24. On November 20, 2023, your affiant identified a white male resembling the physical description of VARNEY exit the **SUBJECT PREMISES**. The white male entered a white vehicle, Oklahoma license plate NXB829. The vehicle drove to Christian Brothers Automotive (CBA), located at 742 Garth Brooks Boulevard, Yukon, Oklahoma 73099. The white male exited the vehicle and entered CBA. The white male exited CBA after some time, and entered a red Toyota Corolla, Oklahoma license plate MNR983. VARNEY is a registered owner of this vehicle along with T.G.

25. Law enforcement personnel have observed the same red Toyota Corolla, Oklahoma license plate MNR983, that VARNEY is a registered owner of at the **SUBJECT PREMISES** on the following dates: November 27, 28, and 29, of 2023. Your affiant believes that the vehicle presence coupled with the received pings, that VARNEY is staying overnight at the **SUBJECT PRESMISES**.

BACKGROUND ON DIGITAL MEDIA STORAGE DEVICES AND CHILD PORNOGRAPHY

26. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. Other digital media storage devices (e.g., compact disks, digital video disks, floppy disks, cell phones, Blackberries, iPhones, thumb drives, video gaming stations, etc.) can also store tremendous amounts of digital information, including digital video and picture files.

27. As is the case with most digital technology, communications by way of computer

can be saved or stored on the computer. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data. Further, even if deleted, forensic examination can sometimes recover files and data including deleted picture files.

28. Computers and other digital file storage devices can store the equivalent of thousands of pages of digital information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires the searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks depending on the volume of the data stored, and it would be generally impossible to accomplish this kind of data search on site. Furthermore, I know that smart cell phones (a type of "computer," as broadly defined in 18 U.S.C. § 1030(e)) can typically "synch" with a traditional desktop or laptop computer. The purpose of synching a smart phone to a traditional computer is to back up data that is stored on the phone so that it is not permanently lost if the portable smart phone is lost or damaged. Also, smart phone users may move files off the smart phone and onto a computer to free up storage space on the smart phone. Similarly, computer (e.g., desktop computers, smart phones, etc.) users may move files off one computer and onto another computer or a digital file storage device such as a thumb drive, a DVD, or an external hard drive, to free up space on the computer. For this reason, I am seeking

authorization to seize all computers and digital file storage devices at the **SUBJECT PREMISES**—not any particular computer.

SPECIFICS OF SEARCH AND SEIZURE OF CELL PHONES AND COMPUTER SYSTEMS

29. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true for the following two reasons:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all of the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover

even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

30. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child exploitation where the evidence frequently includes graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all of the system software (operating systems or interfaces, and hardware drivers) and any application software which may have been used to create the data (whether stored on hard drives or on external media).

31. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, they should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

32. The search procedure for electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully

encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BIOMETRIC ACCESS TO DEVICES

33. I request that this warrant permit law enforcement to compel VARNEY to unlock

any electronic devices requiring biometric access and are subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from the training and experience of other law enforcement officers and my own research, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes, and records data based on the user's facial

characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises, the device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's content. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the content of a device.

f. As discussed in this affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the electronic devices subject to search under this warrant currently is not known

to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the electronic devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials, including those published by device manufacturers, that biometric features will not unlock a device in some circumstances, even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain amount of time. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter any electronic devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, this warrant permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of the occupants of the **SUBJECT PREMISES** to the fingerprint scanner of the electronic devices found at the **SUBJECT PREMISES**; (2) hold the devices found at the **SUBJECT PREMISES** in front of the faces of the occupants of the **SUBJECT**

PREMISES and activate the facial recognition feature; and/or (3) hold the devices found at the **SUBJECT PREMISES** in front of the faces of the occupants of the **SUBJECT PREMISES** and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to require that the occupants of the **SUBJECT PREMISES** state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to require the occupants of the **SUBJECT PREMISES** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

SMARTPHONES

34. Finally, based on the training and the experience of other law enforcement officers and my own research, I know that people who use their computers (including smartphones) to view/access/possess child pornography do so in private to avoid detection. I also know that people who view/access/possess child pornography often use their smartphone. I know smartphones can transfer files back and forth with other computers and digital file storage devices. Files can be stored simultaneously on multiple computers or other digital file storage devices. In the year 2023, smartphone users are almost invariably near their smartphone. Accordingly, I will execute the requested search warrant at a time when I know that Kraig VARNEY is inside the **SUBJECT PREMISES**. If he is inside the **SUBJECT PREMISES**, then his smartphone will almost surely be there too. And I believe there is probable cause that his smartphone, other computer(s), and other digital file storage device(s) will contain evidence of the aforementioned criminal violations, as outlined in detain in Attachment B.

EXECUTION TIME OF THE WARRANT

35. Based on information gathered by law enforcement, I know that VARNEY often leaves for work around 6:15 a.m. To ensure that we are able to execute the warrant at the **SUBJECT PREMISES** when VARNEY is present and with his smartphones or other electronic devices, I am requesting that the search warrant authorize execution in the daytime between 5:30 a.m. to 10:00 p.m.

CONCLUSION

36. Based on the above information, there is probable cause to believe that the foregoing laws have been violated, and that the following property, evidence, fruits, and instrumentalities of these offenses are located at the **SUBJECT PREMISES**.

37. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the **SUBJECT PREMISES**, described in Attachment A, authorizing the seizure of the items described in Attachment B to this Affidavit.

Shane Robinson
Special Agent
Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me this 30th day of November 2023.

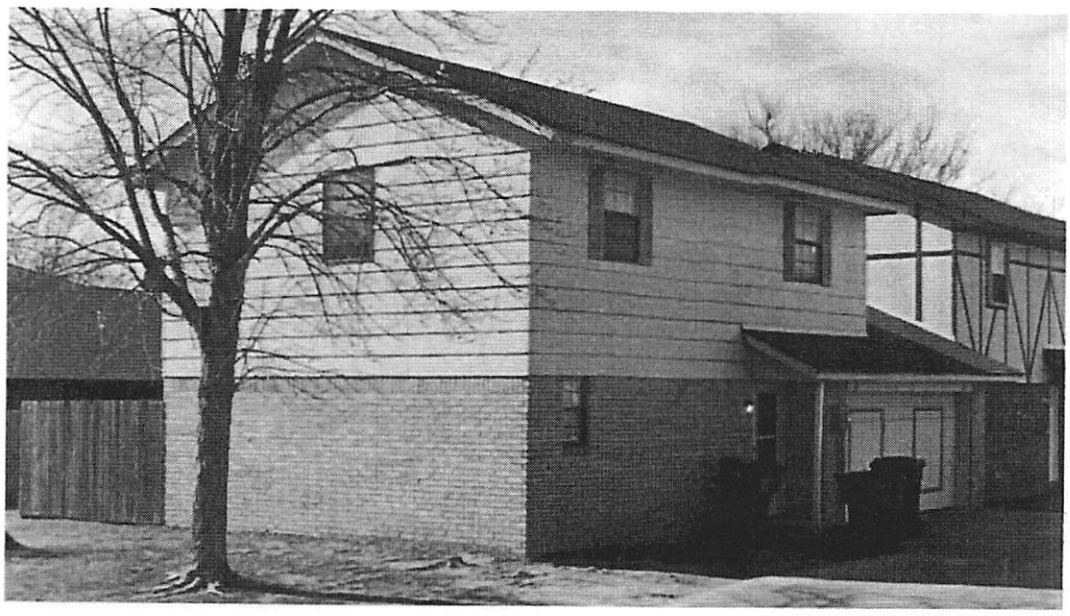
SUZANNE MITCHELL
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PREMISES

8300 NW 10th St., Apt. 2, Oklahoma City, Oklahoma 73127 is a two-story town-home located on the west side of North Davis Avenue. The front exterior of the house is comprised of brown brick and beige panel siding. There are two windows on the second-floor front exterior and one window on the first-floor exterior. An attached two-car garage painted beige with two dark colored rectangles. The residence number "2" is displayed in dark colored numbering over the garage. The area to be searched includes the residence itself as well as any outbuildings, vehicles, and persons within the curtilage of the property.

A photo of the **SUBJECT PREMISES** is below.




NW 10th St
NW 10th St
West River Trail Head Parking
N Davis Ave
LAKEPARK TOWNHOUSES
N Davis Ave
N Eagle Ln
NW 8th St
NW 8th St
NW 8th St
N Davis Ave

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

1. Computer(s), as broadly defined in 18 U.S.C. § 1030(e), other digital file storage devices, computer hardware, computer software, computer-related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that are reasonably believed to have been regularly used by Kraig VARNEY that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography, specifically, for violations of 18 U.S.C. §§ 2252A(a)(2) (receipt and distribution of child pornography) and 2252A(a)(5)(B) (possession of material containing child pornography)—and which are reasonably believed by agents to contain such evidence.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession and distribution of child pornography as defined in 18 U.S.C. § 2256(8).

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium

(including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote

computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

10. Any and all cameras, film, videotapes or other photographic equipment.

11. Any and all visual depictions of minors engaging in sexually explicit conduct.

12. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

13. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

14. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. If law enforcement personnel encounter any electronic devices that are subject to seizure pursuant to this warrant that may be unlocked using a biometric access feature, this warrant

permits law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Kraig VARNEY to the fingerprint scanner of the electronic devices; (2) hold the devices in front of the face of Kraig VARNEY and activate the facial recognition feature; or (3) hold the devices in front of the face of Kraig VARNEY and activate his iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

16. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof or the location of items therein.